NATIONAL SECURITY AGENCY
TECHNOLOGY TRANSFER PROGRAM

Office of Research & Technology Applications

Open Source Software

RELEASES

NSA OSS PORTFOLIO

www.nsa.gov/techtransfer

NSA Technology
Released to Open Source Software

THE TECHNOLOGIES LISTED in this booklet were developed within the National Security Agency (NSA) and are now available to the public via Open Source Software (OSS).

The NSA Technology Transfer Program (TTP) works with agency innovators to transfer their technology from the federal laboratory to the commercial marketplace. This transfer of technology not only fosters ***collaboration and innovation,*** but it also plays a role in strengthening national security by contributing to the nation's ***economic growth.***

To learn more about NSA's OSS technologies or technology licensing opportunities, contact the NSA TTP at tech_transfer@nsa.gov or 866-680-4539.

APACHE **ACCUMULO**

accumulo.apache.org

A sorted, distributed key/value store that provides robust, scalable data storage and retrieval. It adds cell-based access control and a server-side programming mechanism that can modify key/value pairs at various points in the data management process.

APOLLO

Will reside on the NSA github repository

Provides comprehensive static analysis of Android applications for vulnerabilities and malicious behavior.

CASA

www.github.com/iadgov/certificate-authority-situational-awareness

Identifies unexpected and prohibited Certificate Authority certificates on Windows systems.

CONTROL FLOW INTEGRITY RESEARCH

www.github.com/iadgov/control-flow-integrity

A proposed hardware-based method for stopping known memory corruption exploitation techniques described in the “Hardware Control Flow Integrity for an IT Ecosystem” research paper.

DCP

www.github.com/nationalsecurityagency/dcp

A program that reduces the timespan needed for making a forensic copy of hard drives for forensic analysis.

EOWS

Will reside on the NSA github repository

A web enabled prototype tool that implements the Open Checklist Interactive Language (OCIL) capabilities for creating, managing, and responding to questionnaires.

FEMTO

www.github.com/femto-dev/femto

An indexing and search system for queries on sequences of bytes that offers lightning-fast searches on data of arbitrary formats.

GOSECURE

www.github.com/iadgov/gosecure

An easy to use and portable Virtual Private Network system built with Linux and a Raspberry Pi 3.

GRASSMARLIN

www.github.com/iadgov/grassmarlin

Provides network situational awareness of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks to support network security.

JAVA PATHFINDER MANGO (JPF-MANGO)

babelfish.arc.nasa.gov/trac/jpf/wiki/projects/jpf-mango

A static code analysis tool that uses formal methods for analysis. It is part of NASA Ames Java PathFinder project which is a system used to verify executable Java byte code.

LEMONGRAPH/LEMONGRENADE

www.github.com/nationalsecurityagency/lemongraph
www.github.com/nationalsecurityagency/lemongrenade

Log-based transactional graph database engine backed by a single file. The primary use case is to support streaming seed set expansion, iterative correlation, and recursive file processing.

LOCKLEVEL

www.github.com/iadgov/locklevel

A prototype that demonstrates a method for scoring how well Windows systems have implemented some of the top 10 IA mitigation strategies.

MAPLESYRUP

www.github.com/iadgov/maplesyrup

Assesses the security state of an ARM-based device by examining the system register interface of the processor.

NB GALLERY

www.github.com/nbgallery

NB Gallery is a publishing, sharing, and collaboration platform for Jupyter-based analytics.

APACHE NIFI

nifi.apache.org

Automates the flow of data between systems. NiFi implements concepts of Flow-Based Programming and solves common data flow problems faced by enterprises.

ONOP

www.github.com/onop

Radically simplifies the operation of enterprise networks with SDN applications that reside on top of an OpenFlow-capable network controller.

OPAL

Will reside on the NSA github repository

Manages and standardizes existing commercial hard drives.

OPENATTESTATION

www.github.com/openattestation/openattestation

Verifies system integrity by establishing a baseline measurement of a system’s Trusted Platform Module (TPM) and monitors for changes in that measurement. Originally based on NSA’s Host Integrity at Startup (HIS) software.

OZONE TECHNOLOGY

www.github.com/ozoneplatform/owf-framework

A modular suite of “plug and play” services and capabilities, allowing organizations to customize the suite to meet their specific environments.

APACHE PIRK

incubator.apache.org/projects/pirk.html

Enables a user to privately and securely obtain information from a dataset to which they have access without revealing, to the dataset owner or an observer, any information regarding the questions asked or the results obtained.

PRESSUREWAVE

Will reside on the Apache Software Foundation repository

Couples corporate object storage capabilities with a flexible policy language for customization of access control, retention, and storage of data within the same system.

REDHAWK

www.github.com/redhawksdr

A software-defined radio (SDR) framework designed to support the development, deployment, and management of real-time software radio applications.

SAMI

www.github.com/iadgov/splunk-assessment-of-mitigation-implementations

Measures the degree to which specific aspects of the top 10 IA mitigation strategies have been deployed on windows systems.

SCAP SECURITY GUIDE (SSG)

www.fedorahosted.org/scap-security-guide

Delivers security guidance, baselines, and associated validation mechanisms using the Security Content Automation Protocol (SCAP) for hardening Red Hat products.

SECURE HOST BASELINE (SHB)

www.github.com/iadgov/secure-host-baseline

Group Policy Objects, configuration files, compliance checks, and scripts that support implementing the DoD Secure Host Baseline for Windows 10.

SECURITY-ENHANCED LINUX (SELINUX)

www.github.com/selinuxproject

A mandatory access control mechanism in the Linux kernel that checks for allowed operations after standard discretionary access controls are checked. It can enforce rules on files and processes in a Linux system, and on the actions they perform, based on defined policies. SELinux has been part of the Linux kernel since version 2.6.0.

SECURITY ENHANCEMENTS FOR ANDROID (SEANDROID)

source.android.com/security/selinux

Confines privileged processes based on security policies by enforcing mandatory access control over all android processes. SE for Android has been part of Android since Android 4.3.

SIMON AND SPECK

www.github.com/iadgov/simon-speck

The Simon and Speck families of lightweight block ciphers.

SYSTEM INTEGRITY MANAGEMENT PLATFORM (SIMP)

www.github.com/nationalsecurityagency/simp

Automates system configuration and compliance of Linux operating systems so they conform to industry best practices.

TIMELY

www.github.com/nationalsecurityagency/timely

Provides secure access to time series data stored in Accumulo.

UNFETTER

www.github.com/iadgov/unfetter

Provides a mechanism for network defenders, security professionals, and decision makers to quantitatively measure the effectiveness of their security posture.

WALKOFF

www.github.com/iadgov/walkoff

An Active Cyber Defense development framework enabling orchestration capabilities to be written once and then deployed across WALKOFF-enabled orchestration tools.

WATERSLIDE

www.github.com/waterslidelts/waterslide

An architecture for processing metadata designed to take in a set of streaming events from multiple sources, process them through a set of modules, and return meaningful outputs.

WELM

Will reside on the NSA github repository

Retrieves the definitions of Windows Event Log Messages embedded in operating system binaries.

CREATING PARTNERSHIPS

IGNITING INNOVATION

CONTACT US

NSA Office of Research
& Technology Applications
Technology Transfer Program
Research Directorate

9800 Savage Road, Suite 6843
Ft. Meade, MD 20755-6843

(866) 680-4539
tech_transfer@nsa.gov
www.nsa.gov/techtransfer